1972

Gaussian Pythagorean Triples

Joyce G. Ramige

Gaussian Pythagorean Triples

By

Joyce G. Ramige

A thesis submitted
in partial fulfillment of the requirements for the
degree Master of Science, Major in
Mathematics, South Dakota
State University

1972

Gaussian Pythagorean Triples

This thesis is approved as a creditable and independent investigation by a candidate for the degree, Master of Science, and is acceptable for meeting the thesis requirements for this degree. Acceptance of this thesis does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department.

Thesis Adviser Date

Head, Mathematics Dept. Date

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to Dr. G. E. Bergum of the Mathematics Department for the time and effort he afforded to put this thesis in its final form. Thanks are also given to Professor Milo F. Bryn for reading the manuscript and making many helpful suggestions.

JGR

TABLE OF CONTENTS

I. Introduction

For positive integers a, b, c, we call the ordered triple (a, b, c) a Pythagorean triple provided $a^2 + b^2 = c^2$. A Pythagorean triple is said to be primitive if a and b are relatively prime. It is a well-known fact [2, pp. 127-130] that a primitive Pythagorean triple (a, b, c) in which a is even can be represented by $a = 2xy$, $b = x^2 - y^2$, $c = x^2 + y^2$, where x and y are positive integers. Teigen and Hadwin [4] note that it is not possible to represent all Pythagorean triples in this way. In particular, they observe that (12, 9, 15) does not have such a representation. Furthermore, Teigen and Hadwin present a new way of representing and generating all Pythagorean triples. In [4], we find

Theorem 1.1. Suppose (a, b, c) is a Pythagorean triple. If x, y, z are defined by

(1) $\qquad x = c - b, \quad y = c - a, \quad z = a + b - c,$

then a, b, c may be represented in the form

(2) $\qquad a = x + z, \quad b = y + z, \quad c = x + y + z,$

where x, y, z satisfy

(3) $\qquad$ x, y, z are positive, $\quad 2xy = z^2, \quad$ z is even.

Conversely, if x, y, z are integers satisfying (3) and a, b, c are defined by (2), then (a, b, c) is a Pythagorean triple satisfying (1).

Theorem 1.2. Let a, b, c, x, y, z be as in Theorem 1.1. Then a and b are relatively prime iff x and y are relatively prime.

More current results, which also involve the idea of generating Pythagorean triples, are found in [1]. They are

Theorem 1.3. Let (a, b, c) be a Pythagorean triple and d = c - b. For a positive integer n, define $a_1 = a$, $b_1 = b$, $c_1 = c$ and $a_n = a_{n-1} + 2d$, $b_n = a_n + a_{n-1} + b_{n-1}$, $c_n = b_n + d$. Then (a_n, b_n, c_n) is a Pythagorean triple. Further, if (a, b, c) is a primitive triple, then (a_n, b_n, c_n) is a primitive triple.

and

Theorem 1.4. Let (a, b, c) be a Pythagorean triple and d = c - b. For a positive integer n, define $a_1 = a$, $b_1 = b$, $c_1 = c$ and $a_n = a_{n-1} + d$, $b_n = a_{n-1} + b_{n-1} + d/2$, $c_n = b_n + d$. Then (a_n, b_n, c_n) is a Pythagorean triple for all n. Further, if d/2 is even and (a, b, c) is primitive, then (a_n, b_n, c_n) is a primitive triple for all n.

The purpose of this paper is to generalize the well-known results about Pythagorean triples as well as the results of Teigen and Hadwin [4] and Arpaia [1] to the Euclidean domain of the Gaussian integers, which we denote by Z(i), where $Z(i)=\{a + bi \mid a, b \in Z\}$ with Z the set of rational integers.

Throughout the remainder of this paper, unless stated otherwise, the letters of the Greek alphabet will be used to represent integers in

the integral domain $Z(i)$. In particular, the Greek letters ρ_i and π_i will represent primes in $Z(i)$. Latin letters with the exception of i, which is the imaginary unit for the complex number system, will represent rational integers.

For $\alpha = a + bi$, we define the conjugate as $\bar{\alpha} = a - bi$ and the norm of α as $N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$. We say that $\alpha \neq 0$ divides β and write $\alpha|\beta$ iff there exists γ such that $\beta = \alpha\gamma$. Furthermore, α is a unit iff α has a multiplicative inverse or equivalently iff $\alpha|\beta$ for all β in $Z(i)$. An element ρ in $Z(i)$ is prime iff $\rho = \alpha\beta$ implies that either α or β is a unit but not both. Trivially, the norm of a product is the product of the norms so that the norm is multiplicative. Using this result, it can be shown that α is a unit iff $N(\alpha) = 1$; hence, the units of $Z(i)$ are ± 1 and $\pm i$. We say that α and β are associates iff $\alpha = \beta\varepsilon$, where ε is a unit of $Z(i)$.

Since $Z(i)$ is a Euclidean domain, we have

Theorem 1.5. If α and $\beta \neq 0$ are in $Z(i)$, then there exist γ and δ in $Z(i)$ such that $\alpha = \beta\gamma + \delta$, where $N(\delta) < N(\beta)$.

An immediate consequence of Theorem 1.5 is that $Z(i)$ is a unique factorization domain so that every element can be written as a product of primes and the representation is unique to within units and order of the factors.

If there exists a δ such that $\delta|\alpha$ and $\delta|\beta$, and $\gamma|\delta$ whenever $\gamma|\alpha$ and $\gamma|\beta$, then δ is called the greatest common divisor (g.c.d.) of α and β and we write $(\alpha,\beta) = \delta$. Observe that the g.c.d. is unique up to

associates. In particular, if $(\alpha,\beta) = \varepsilon$, where ε is a unit, we will write $(\alpha,\beta) = 1$ and say that α and β are relatively prime. Since $Z(i)$ is a Euclidean domain, every pair of Gaussian integers, not both zero, has a g.c.d., and if $(\alpha,\beta) = \delta$ there exist σ_1 and σ_2 such that $\alpha\sigma_1 + \beta\sigma_2 = \delta$.

II. A Generalization of an Old Result

We shall say that the ordered triple (α, β, γ) is a Gaussian Pythagorean triple (G.P.T.) iff $\alpha^2 + \beta^2 = \gamma^2$. First note that we may as well assume α and β are relatively prime. Suppose $(\alpha, \beta) = \delta \neq 1$. Then there exist Gaussian integers σ_1 and σ_2 such that $\alpha\sigma_1 + \beta\sigma_2 = \delta$. Therefore, $(\alpha/\delta)\sigma_1 + (\beta/\delta)\sigma_2 = 1$ so that $(\alpha/\delta, \beta/\delta) = 1$. Furthermore, $\delta|\gamma$ and $(\alpha/\delta)^2 + (\beta/\delta)^2 = (\gamma/\delta)^2$. Conversely, if (α, β, γ) is a G.P.T. so is $(\alpha\delta, \beta\delta, \gamma\delta)$ for any δ. We call (α, β, γ) a primitive Gaussian Pythagorean triple (P.G.P.T.) iff $(\alpha, \beta) = 1$. We also observe that if $\alpha^2 + \beta^2 = \gamma^2$, then

(a) $$\overline{\alpha}^2 + \overline{\beta}^2 = \overline{\gamma}^2$$

(b) $$(i\alpha)^2 + (i\beta)^2 = (i\gamma)^2$$

(c) $$(-\alpha)^2 + (-\beta)^2 = (-\gamma)^2$$

(d) $$(-\alpha)^2 + \beta^2 = (-\gamma)^2$$

(e) $$\alpha^2 + (-\beta)^2 = \gamma^2.$$

In fact, there are 32 different possible triples that one can obtain from a given triple. The proof that each of the 32 triples is Pythagorean is immediate and hence omitted. Throughout the remainder of this paper, we will assume that α, β, and γ are on or to the right of the y-axis.

In Jordan [3], we find the following:

Definition 2.1. A Gaussian integer γ is even iff $(1 + i)|\gamma$.

The purpose of this section is to prove the following theorem:

Theorem 2.1. The ordered triple (α, β, γ) is a P.G.P.T., where $2|\alpha$, iff there exist Gaussian integers σ_1 and σ_2 such that

(1) $$(\sigma_1, \sigma_2) = 1,$$

(2) not both σ_1 and σ_2 are odd,

and

(3) $$\alpha = 2\varepsilon\sigma_1\sigma_2, \quad \beta = \varepsilon_1\sigma_1^2 - \varepsilon_2\sigma_2^2, \quad \gamma = \varepsilon_1\sigma_1^2 + \varepsilon_2\sigma_2^2,$$

where $\varepsilon^2 = \varepsilon_1\varepsilon_2 = \pm 1$.

In order to prove Theorem 2.1, it is convenient to establish the following lemmas:

Lemma 2.1. If $(\alpha, \beta) = 1$ and $\alpha^2 + \beta^2 = \gamma^2$, then $(\alpha, \gamma) = (\beta, \gamma) = 1$.

Proof.--Suppose $(\alpha, \gamma) = \delta$, where δ is some integer other than a unit. Since $Z(i)$ is a unique factorization domain, there exists a prime ρ such that $\rho|\delta$. Hence, $\rho|\alpha$ and $\rho|\gamma$ so that $\rho|\alpha^2$ and $\rho|\gamma^2$ or $\rho|(\alpha^2 - \gamma^2)$. But $\gamma^2 - \alpha^2 = \beta^2$ so $\rho|\beta^2$ or $\rho|\beta$. This is contrary to $(\alpha, \beta) = 1$. Thus, $(\alpha, \gamma) = 1$. Similarly, one can show that $(\beta, \gamma) = 1$.

Lemma 2.2. By the division algorithm, $\alpha = 2\delta + \theta$, where $N(\theta) < 4$. We can assume without loss of generality that $\theta = 0, 1, i, 1 + i$.

Proof.--Since $N(\theta) < 4$, $N(\theta) = 0, 1, 2, 3$. But $N(\theta) = 3$ is impossible. Therefore, $N(\theta) = 0, 1$, or 2. If $N(\theta) = 0$, then $\theta = 0$.

If $N(\theta) = 1$, then $\theta = \pm 1, \pm i$. Let $\theta = -1$, then $\alpha = 2\delta - 1 = 2(\delta - 1) + 1 = 2\delta_1 + 1$. Let $\theta = -i$, then $2\delta - i = 2(\delta - i) + i = 2\delta_2 + i$. If $N(\theta) = 2$, then $\theta = \pm 1 \pm i$. By an argument similar to the above, we have $\alpha = 2\delta_3 + (1 + i)$ for some δ_3 if $\theta = \pm 1 \pm i$.

Since γ is even iff $(1 + i)|\gamma$, we see from Lemma 2.2 that a Gaussian integer is odd iff it is of the form $2\theta + i$ or $2\theta + 1$.

Now we would hope, as is the case with the rational integers, that if (α, β, γ) is a P.G.P.T., then exactly one of α or β is divisible by two. It can be shown by a counter example that this is not true for if $\alpha = -7 + 6i$ and $\beta = 6 + 9i$, then $\gamma^2 = \alpha^2 + \beta^2 = (2 + 6i)^2$. In fact, we will exhibit a family of primitive Gaussian Pythagorean triples, where α is of the form $2\theta + 1$ and β is of the form $2\theta_1 + i$.

Theorem 2.2: The ordered triple (α, β, γ) is a P.G.P.T., γ - even, iff there exist integers $a = 2n$ and $b = 2m$ such that

$$\alpha = (1 - 4mn) + 2(n^2 - m^2)i$$

and

$$\beta = 2(n^2 - m^2) + (1 + 4mn)i.$$

Proof.--We shall first show that the sufficient conditions of the theorem are satisfied. Before doing this, we observe that α is of the form $2\theta + 1$ and β is of the form $2\theta_1 + i$ for some θ_1, θ. It can be shown by direct calculation that

$$\alpha^2 + \beta^2 = 8i(n + mi)^2 = (1 + i)^2 (a + bi)^2.$$

Let $\gamma = (1 + i)(a + bi)$. Then $\alpha^2 + \beta^2 = \gamma^2$ and $(1 + i) | \gamma$. If $(\alpha, \beta, \gamma) \neq 1$, then there exists a δ such that $\delta | \alpha$ and $\delta | \beta$. Hence, $\delta | (i\alpha + \beta)$. Since $i\alpha + \beta = 2i = (1 + i)^2$, the only possibilities for δ are ε, 2ε, $(1 + i)\varepsilon$, where ε is a unit. Since α and β are both odd, δ is a unit and the conditions are sufficient.

Conversely, let γ be even. Then $\gamma = (1 + i)(a + bi) = (a - b) + (a + b)i$ so that $\alpha^2 + \beta^2 = -4ab + 2i(a^2 - b^2)$. If α and β are to have the desired form, then $-4ab + 2i(a^2 - b^2) = 8i(n + mi)^2$. Hence, $4mn = ab$ and $4(n^2 - m^2) = a^2 - b^2$ from which we conclude that both a and b are divisible by two. Let $a = 2n$ and $b = 2m$. Since $\alpha^2 + \beta^2 = (\alpha + \beta i)(\alpha - \beta i)$, we will let $\alpha + \beta i = -2ab + (a^2 - b^2)i$ and $\alpha - \beta i = 2$. Solving for α and β, we obtain

$$\alpha = (1 - 4mn) + (4n^2 - 4m^2)i/2 = (1 - 4mn) + (2n^2 - 2m^2)i$$

and

$$\beta = (-i - 4nmi)/i^2 + (4n^2 - 4m^2)/2 = 2(n^2 - m^2) + i(1 + 4mn).$$

This family of primitive Gaussian Pythagorean triples for which $2 \nmid \alpha$ and $2 \nmid \beta$ and of which our counter example is a member does not cause us any serious difficulty if we use the properties of i. To eliminate the difficulty, we have

Lemma 2.3. If (α, β, γ) is a P.G.P.T., then we can assume without loss of generality that exactly one of α or β is divisible by two.

Before giving the details of the proof for Lemma 2.3, we introduce the concept of congruence modulo a Gaussian integer. In [2, p. 161], we find

Definition 2.2. Two Gaussian integers α and β are said to be congruent modulo γ iff the difference $\alpha - \beta$ is divisible by γ. We write $\alpha \equiv \beta \pmod{\gamma}$.

Proof of Lemma 2.3.--By Lemma 2.2, $\alpha = 2\theta + 0, 2\theta + 1, 2\theta + i$, or $2\theta + (i + 1)$ so that

$$\alpha^2 \equiv 0, 1, 3, 2i \pmod 4. \tag{1}$$

Using symmetry and the fact that $(\alpha, \beta) = 1$, we need only consider the following pairs of remainders:

	α	β	α^2	β^2	$\alpha^2 + \beta^2 \pmod 4$
(a)	0	1	0	1	1
(b)	0	i	0	-1	3
(c)	1	i	1	-1	0
(d)	1	1	1	1	2
(e)	1	1 + i	1	2i	1 + 2i
(f)	i	i	-1	-1	2
(g)	i	1 + i	-1	2i	2i + 3

By (1), we can eliminate cases (d) - (g). If $\alpha = 2\theta + 1$ and $\beta = 2\theta_1 + i$ as in (c), then γ must be of the form $2\theta_2$. But $\alpha^2 = \gamma^2 - \beta^2 = \gamma^2 + (i\beta)^2$, where $i\beta$ is of the form $2\theta_3 + 1$. Thus, we have case (a) where γ now assumes the role of α. Using $\beta^2 = \gamma^2 + (i\alpha)^2$, we obtain a similar result. Therefore, we can assume without loss of generality that $2|\alpha$, and β is of the form $2\theta_1 + 1$ or $2\theta_1 + i$.

Henceforth, we will assume that $2|\alpha$ if (α, β, γ) is a P.G.P.T.

Lemma 2.4. If (α, β, γ) is a P.G.P.T., then both β and γ are odd.

Proof.--Since α is even and $(\alpha, \beta) = 1$, neither γ nor β can be divisible by $1 + i$. Hence, they are both odd.

Because β and γ are both odd in a P.G.P.T. and since there are two forms for odd Gaussian integers, we establish the following:

Lemma 2.5. If (α, β, γ) is a P.G.P.T., then $\beta \equiv \gamma \pmod 2$.

Proof.--Since (α, β, γ) is a P.G.P.T., $\alpha = 2\theta_1$. Let $\beta = 2\theta_2 + 1$. Then $\alpha^2 + \beta^2$ is of the form $4\theta_3 + 1$. If $\gamma = 2\theta_4 + i$, then $\gamma^2 = 4\theta_5 - 1$ so that $4\theta_3 + 1 = 4\theta_5 - 1$ or $\theta_3 - \theta_5 = -1/2$, which is impossible since θ_3 and θ_5 are Gaussian integers. Hence, γ is of the form $2\theta_4 + 1$ and $\beta \equiv \gamma \pmod 2$. Similarly, if β is of the form $2\theta_2 + i$, we must have γ of the form $2\theta_4 + i$ and thus, $\beta \equiv \gamma \pmod 2$.

In order to prove that the conditions of Theorem 2.1 are necessary and sufficient, we need only establish one more lemma.

Lemma 2.6. If $\alpha\beta = \gamma^2$ and $(\alpha, \beta) = 1$, then both α and β are perfect squares up to units.

Proof.--Let the prime-power decompositions of α and β be

$$\alpha = \varepsilon_1 \rho_1^{e_1} \rho_2^{e_2} \cdots \rho_k^{e_k}$$

and

$$\beta = \varepsilon_2 \pi_1^{f_1} \pi_2^{f_2} \cdots \pi_j^{f_j},$$

where ε_1, ε_2 are units and in each decomposition no two of the primes are associates. From $(\alpha, \beta) = 1$, it follows that no prime appears in both decompositions. Because $Z(i)$ is a unique factorization domain, the prime-power decomposition of γ^2 can be written as

$$\gamma^2 = \alpha\beta = \varepsilon_1\varepsilon_2\rho_1^{e_1}\rho_2^{e_2}\ldots\rho_k^{e_k}\pi_1^{f_1}\pi_2^{f_2}\ldots\pi_j^{f_j}.$$

Since γ^2 is a square, all of the exponents $e_1, e_2, \ldots e_k, f_1, f_2 \ldots f_k$ are even. Thus, α and β are squares up to units. Note that $\varepsilon_1\varepsilon_2 = \pm 1$.

Theorem 2.3. If (α, β, γ) is a P.G.P.T., then there exist Gaussian integers σ_1 and σ_2 such that $(\sigma_1, \sigma_2) = 1$, not both σ_1 and σ_2 are odd, and $\alpha = 2\varepsilon\sigma_1\sigma_2$, $\beta = \varepsilon_1\sigma_1^2 - \varepsilon_2\sigma_2^2$, $\gamma = \varepsilon_1\sigma_1^2 + \varepsilon_2\sigma_2^2$, where $\varepsilon^2 = \varepsilon_1\varepsilon_2 = \pm 1$.

Proof.--Since α is divisible by two, $\alpha = 2\theta$ for some θ or $\alpha^2 = 4\theta^2$. From $\alpha^2 = \gamma^2 - \beta^2$ we have

(1) $$4\theta^2 = (\gamma - \beta)(\gamma + \beta).$$

By Lemma 2.5

(2) $$\gamma + \beta = 2\phi \quad \text{and} \quad \gamma - \beta = 2\tau.$$

Therefore,

(3) $$\gamma = \phi + \tau \quad \text{and} \quad \beta = \phi - \tau.$$

Substituting (2) into (1), we get

$$4\theta^2 = (2\phi)(2\tau) \text{ or } \theta^2 = \phi\tau.$$

If ϕ and τ are relatively prime, we can apply Lemma 2.6 and conclude

that ϕ and τ are both perfect squares up to units. In fact, ϕ and τ are relatively prime, as we now show. Suppose that $\delta|\phi$ and $\delta|\tau$. From (3), it follows that $\delta|\gamma$ and $\delta|\beta$. But we know that $(\gamma, \beta) = 1$. Hence, $\delta = \pm 1, \pm i$ and $(\phi, \tau) = 1$. By Lemma 2.6 we have $\phi = \varepsilon_1\sigma_1^2$ and $\tau = \varepsilon_2\sigma_2^2$ for some integers σ_1 and σ_2, where $\varepsilon_1\varepsilon_2 = \pm 1$. Thus,

$$\alpha^2 = 4\theta^2 = 4\phi\tau = \pm 4\sigma_1^2\sigma_2^2 \text{ or } \alpha = 2\varepsilon\sigma_1\sigma_2,$$

where $\varepsilon^2 = \pm 1$. From (3),

$$\gamma = \phi + \tau = \varepsilon_1\sigma_1^2 + \varepsilon_2\sigma_2^2$$

and

$$\beta = \phi - \tau = \varepsilon_1\sigma_1^2 - \varepsilon_2\sigma_2^2.$$

Having established the last three equations, we need now only show that $(\sigma_1, \sigma_2) = 1$ and not both σ_1 and σ_2 are odd. Let $\delta|\sigma_1$ and $\delta|\sigma_2$. Then $\delta|\alpha$ and $\delta|\beta$. Hence, $\delta = \varepsilon$, where ε is a unit, because $(\alpha, \beta) = 1$. If $(\sigma_1, \sigma_2) = 1$, it follows that σ_1 and σ_2 cannot both be even. Suppose they are both odd. This is contrary to γ, β are odd. Therefore, exactly one of σ_1 and σ_2 is odd.

Theorem 2.4. If there exist Gaussian integers σ_1 and σ_2 such that $(\sigma_1, \sigma_2) = 1$, not both σ_1 and σ_2 are odd, and $\alpha = 2\varepsilon\sigma_1\sigma_2$, $\beta = \varepsilon_1\sigma_1^2 - \varepsilon_2\sigma_2^2$, $\gamma = \varepsilon_1\sigma_1^2 + \varepsilon_2\sigma_2^2$, where $\varepsilon^2 = \varepsilon_1\varepsilon_2 = \pm 1$, then (α, β, γ) is a P.G.P.T.

Proof.--By hypothesis,

$$\alpha^2 + \beta^2 = 4\varepsilon^2\sigma_1^2\sigma_2^2 + \varepsilon_1^2\sigma_1^4 - 2\varepsilon^2\sigma_1^2\sigma_2^2 + \varepsilon_2^2\sigma_2^4$$

$$= \varepsilon_1^2\sigma_1^4 + 2\varepsilon^2\sigma_1^2\sigma_2^2 + \varepsilon_2^2\sigma_2^4$$

$$= (\varepsilon_1\sigma_1^2 + \varepsilon_2\sigma_2^2)^2$$

$$= \gamma^2.$$

It remains to be shown that $(\alpha, \beta, \gamma) = 1$. Suppose ρ is an odd prime such that $\rho|\alpha$ and $\rho|\beta$. From $\gamma^2 = \alpha^2 + \beta^2$, it follows that $\rho|\gamma$. From $\rho|\beta$ and $\rho|\gamma$ it follows that $\rho|(\beta + \gamma)$ and $\rho|(\beta - \gamma)$. But $\beta + \gamma = 2\varepsilon_1\sigma_1^2$ and $\beta - \gamma = -2\varepsilon_2\sigma_2^2$. So $\rho|2\sigma_1^2$ and $\rho|2\sigma_2^2$. Since ρ is odd, we conclude that $\rho|\sigma_1^2$ and $\rho|\sigma_2^2$. Hence, $\rho|\sigma_1$ and $\rho|\sigma_2$. This is contrary to $(\sigma_1, \sigma_2) = 1$. The only other way in which α and β could fail to be relatively prime is for both to be divisible by $1 + i$. But β is odd because $\beta = \varepsilon_1\sigma_1^2 - \varepsilon_2\sigma_2^2$ and one of σ_1 or σ_2 is even and the other is odd. Thus, $(\alpha, \beta) = 1$ and (α, β, γ) is a P.G.P.T.

Combining Theorems 2.3 and 2.4, we have the desired results; therefore, Theorem 2.1 is proved.

III. Other Ways of Generating Pythagorean Triples

In this section, we shall first generalize the results of Teigen and Hadwin [4] to $Z(i)$.

Theorem 3.1. The ordered triple (α, β, γ) is a G.P.T. iff there exist σ, τ, δ such that $2\sigma\tau = \delta^2$, $2|\delta$, where $\alpha = \sigma + \delta$, $\beta = \tau + \delta$, and $\gamma = \sigma + \tau + \delta$.

Proof.--Suppose $\alpha^2 + \beta^2 = \gamma^2$. Let

(1) $\tau = \gamma - \alpha, \quad \delta = \alpha + \beta - \gamma, \quad \sigma = \gamma - \beta.$

Solving for α, β, and γ, we have

(2) $\alpha = \sigma + \delta, \quad \beta = \tau + \delta, \quad \gamma = \sigma + \tau + \delta,$

where $2\sigma\tau = \delta^2$ since

$$\begin{aligned} 2\sigma\tau &= 2(\gamma - \beta)(\gamma - \alpha) \\ &= 2(\gamma^2 - \beta\gamma - \alpha\gamma + \beta\alpha) \\ &= \gamma^2 + \gamma^2 - 2\beta\gamma - 2\alpha\gamma + 2\beta\alpha \\ &= \alpha^2 + \beta^2 + \gamma^2 - 2\beta\gamma - 2\alpha\gamma + 2\beta\alpha \\ &= (\alpha + \beta - \gamma)^2 \\ &= \delta^2. \end{aligned}$$

Since $2|\alpha$ and $2|(\beta - \gamma)$, we have $2|(\alpha + \beta - \gamma)$ or $2|\delta$.

Conversely, suppose $2\sigma\tau = \delta^2$, $2|\delta$, where $\alpha = \sigma + \delta$, $\beta = \tau + \delta$, and $\gamma = \sigma + \tau + \delta$. It follows that

$$\begin{aligned} \alpha^2 + \beta^2 &= (\sigma + \delta)^2 + (\tau + \delta)^2 \\ &= \sigma^2 + 2\sigma\delta + \delta^2 + \tau^2 + 2\tau\delta + \delta^2. \end{aligned}$$

Substituting $\delta^2 = 2\sigma\tau$, we have

$$\alpha^2 + \beta^2 = \sigma^2 + 2\sigma\delta + 2\sigma\tau + \tau^2 + 2\delta\tau + \delta^2$$
$$= (\sigma + \tau + \delta)^2.$$

Hence, (α, β, γ) is a G.P.T.

Theorem 3.1 tells us that we may generate any G.P.T. by choosing an integer δ divisible by 2, an integer σ which is a factor of $\delta^2/2$, and letting $\tau = \delta^2/2\sigma$. It follows from (1) that the representation of the triple (α, β, γ) in terms of σ, τ, δ is unique. Thus, each G.P.T. is generated exactly once by this method.

The following theorem presents a new way of generating a P.G.P.T.

Theorem 3.2. Let α, β, γ, σ, τ, δ be as in Theorem 3.1. Then α and β are relatively prime iff σ and τ are relatively prime.

Proof.--Suppose α and β are relatively prime. Since $2\sigma\tau = \delta^2$, any factor common to σ and τ is necessarily a factor of δ. From $\alpha = \delta + \sigma$ and $\beta = \delta + \tau$, it follows that any factor common to σ and τ must also be a common factor of α and β. Since α and β are relatively prime, σ and τ must also be relatively prime.

Conversely, suppose that σ and τ are relatively prime. It follows from $2\sigma\tau = \delta^2$ that there are relatively prime Gaussian integers 2θ and ϕ which, we can assume without loss of generality, are such that $\sigma = 2\varepsilon_1\theta^2$, $\tau = \varepsilon_2\phi^2$, and $\delta = 2\varepsilon_3\theta\phi$ with ε_1, ε_2, ε_3 units. Thus,

$\alpha = \sigma + \delta = 2\varepsilon_1\theta^2 + 2\varepsilon_3\theta\phi = 2\theta(\varepsilon_1\theta + \varepsilon_3\phi)$ and

$$\beta = \tau + \delta = \varepsilon_2\phi^2 + 2\varepsilon_3\theta\phi = \phi(\varepsilon_2\phi + 2\varepsilon_3\theta).$$

To prove that α and β are relatively prime it suffices to show that each of the terms 2θ, $\theta + \phi$ is relatively prime to the terms ϕ, $\phi + 2\theta$. We shall show that $\theta + \phi$ and $2\theta + \phi$ are relatively prime. It follows from $2\theta = 2(\phi + 2\theta) - 2(\theta + \phi)$ and $\phi = 2(\theta + \phi) - (\phi + 2\theta)$ that any factor common to $\theta + \phi$ and $2\theta + \phi$ also must be a common factor of $2\varepsilon_1\theta$ and $\varepsilon_2\phi$. Since $2\varepsilon_1\theta$ and $\varepsilon_2\phi$ are relatively prime, $\theta + \phi$ and $\phi + 2\theta$ must be relatively prime.

Theorem 3.3. Let (α, β, γ) be a G.P.T. and $\delta = \gamma - \beta$. For a positive rational integer n, define $\alpha_1 = \alpha$, $\beta_1 = \beta$, $\gamma_1 = \gamma$ and $\alpha_n = \alpha_{n-1} + 2\delta$, $\beta_n = \alpha_n + \alpha_{n-1} + \beta_{n-1}$, $\gamma_n = \beta_n + \delta$. Then $(\alpha_n, \beta_n, \gamma_n)$ is a G.P.T. Further, if (α, β, γ) is a P.G.P.T., then $(\alpha_n, \beta_n, \gamma_n)$ is a P.G.P.T.

Proof.--If n = 1 the proposition is trivially true. Suppose that the proposition is true for all positive k less than n. Now $\alpha_n^2 + \beta_n^2 = (\alpha_{n-1} + 2\delta)^2 + (2\alpha_{n-1} + \beta_{n-1} + 2\delta)^2$. On expanding, rearranging terms and using the fact $\alpha_{n-1}^2 + \beta_{n-1}^2 = \gamma_{n-1}^2 = (\beta_{n-1} + \delta)^2$ we have $\alpha_n^2 + \beta_n^2 = \gamma_n^2$. Now suppose that for some positive k, $(\alpha_k, \beta_k, \gamma_k)$ is not a P.G.P.T. while (α, β, γ) is a P.G.P.T. Let ρ be any prime divisor of α_k, β_k, γ_k. Since $\delta = \gamma_k - \beta_k$, ρ divides δ. Further, since $\alpha_{k-1} = \alpha_k - 2\delta$, ρ divides α_{k-1}. But then ρ divides β_{k-1} since $\beta_{k-1} = \beta_k - (\alpha_{k-1} + \alpha_k)$. Finally, since $\gamma_{k-1} = \beta_{k-1} + \delta$,

ρ divides γ_{k-1}. Surely then ρ divides each of α, β, γ contradicting our hypothesis.

Theorem 3.4. Let (α, β, γ) be a G.P.T. and $\delta = \gamma - \beta$. For a positive rational integer n, define $\alpha_1 = \alpha$, $\beta_1 = \beta$, $\gamma_1 = \gamma$ and $\alpha_n = \alpha_{n-1} + \delta$, $\beta_n = \alpha_{n-1} + \beta_{n-1} + \delta/2$, $\gamma_n = \beta_n + \delta$. Then $(\alpha_n, \beta_n, \gamma_n)$ is a G.P.T. for all n. Further, if $\delta/2$ is even and (α, β, γ) is a P.G.P.T., then $(\alpha_n, \beta_n, \gamma_n)$ is a P.G.P.T. for all n.

Proof.--If n = 1 the proposition is trivially true. Hence, suppose that the proposition is true for all positive k less than n. Now $\alpha_n^2 + \beta_n^2 = (\alpha_{n-1} + \delta)^2 + (\alpha_{n-1} + \beta_{n-1} + \delta/2)^2$. On expanding, rearranging terms and using the fact that $\alpha_{n-1}^2 + \beta_{n-1}^2 = \gamma_{n-1}^2 = (\beta_{n-1} + \delta)^2$ we have $\alpha_n^2 + \beta_n^2 = \gamma_n^2$. Now suppose that for positive k, $(\alpha_k, \beta_k, \gamma_k)$ is not a P.G.P.T. while (α, β, γ) is a P.G.P.T. and $\delta/2$ is even. Let ρ be any prime divisor of α_k, β_k, γ_k. Now ρ divides δ and ρ divides α_{k-1}. If ρ is odd, then ρ divides $\delta/2$. Hence, ρ divides β_{k-1}. But then ρ divides γ_{k-1}. Hence, surely ρ divides α, β, γ contradicting our hypothesis. If $\rho = 1 + i$ and $\delta/2$ is even, then $1 + i$ divides β_{k-1} since $\beta_{k-1} = \beta_k - (\alpha_{k-1} + \delta/2)$. But then $1 + i$ divides γ_{k-1}. Therefore we conclude that $1 + i$ divides α, β, γ, but that is contrary to $(\alpha, \beta, \gamma) = 1$.

In conclusion, we observe that if (α, β, γ) and $(\alpha_1, \beta_1, \gamma_1)$ are G.P.T., then $((\alpha\alpha_1 - \beta\beta_1), (\alpha\beta_1 + \beta\alpha_1), \gamma\gamma_1)$ is a G.P.T. Since the details are straightforward, they are left to the reader.

REFERENCES

1. P. J. Arpaia, A generating property of Pythagorean triples, Mathematics Magazine, 44(1971) 26-27.

2. I. A. Barnett, Elements of Number Theory, Prindle, Weber and Schmidt, incorporated, Boston, 1969.

3. C. A. Holben and J. H. Jordan, The twin prime problem and Goldbach's Conjecture in the Gaussian integers, The Fibonacci Quarterly, 8(1968)81.

4. M. G. Teigen and D. W. Hadwin, On generating Pythagorean triples, The American Mathematical Monthly, 78(1971) 378-379.